What Is Claimed Is:

1. A method that facilitates secure electronic commerce, comprising:

providing a consumer with a file of security data relating to an account maintained by a financial institution;

creating a financial transaction between the consumer and a merchant, wherein the financial transaction is protected using security data from the file, and wherein the financial transaction is structured to contain an account number in a form that is undecipherable by the merchant, thereby prevent the merchant from knowing the account number for the account;

validating by the merchant that the financial institution identified by the financial transaction is acceptable using security data from the file;

requesting by the merchant that the financial institution authorize the financial transaction;

receiving by the merchant an authorization from the financial institution to complete the financial transaction;

completing the financial transaction between the consumer and the merchant; and

notifying the financial institution that the financial transaction is complete.

2. The method of claim 1, wherein the file of security data includes:

a consumer identifier;

a private key for encryption and authentication of data;

a first public key related to the private key for decryption and authentication of data;

an identifier identifying the financial institution;

a second public key belonging to the financial institution;

the account number that has been encrypted with a key known only to the financial institution creating an encrypted account number;

a first certificate signed by a recognized certificate authority that validates the financial institution;

a second certificate signed by the financial institution that validates the consumer; and

computer algorithms to use the file of security data.

3. The method of claim 2, wherein the file of security data is provided to the consumer on a smart card.

4. The method of claim 3, wherein protecting the financial transaction involves:

creating a first hash of the financial transaction; and

encrypting the first hash, the second certificate, and the encrypted account number using the second public key creating a secure envelope of transaction data, wherein the first hash is created at a secure site available only to the consumer.

5. The method of claim 4, wherein requesting by the merchant that the financial institution authorize the financial transaction involves:

creating a second hash of the financial transaction by the merchant;

sending the secure envelope and the second hash to the financial institution;

decrypting at the financial institution the secure envelope using the private key of the financial institution;

comparing the first hash with the second hash; and if the first hash is identical to the second hash,

decrypting the encrypted account number to recover the account number for the account belonging to the consumer,

verifying that the financial transaction is valid for the account, and

if valid, authorizing the financial transaction.

6. The method of claim 5, wherein verifying that the financial transaction is valid for the account includes:

verifying that the second certificate was signed by the financial institution;

determining that the account is valid; and

ensuring that a transaction amount is not greater than an authorized transaction amount.

7. The method of claim 4, wherein the secure site available only to the consumer is within the smart card.

8. The method of claim 2, wherein validating by the merchant that the financial institution identified by the financial transaction is acceptable involves:

receiving at the merchant the first certificate; and

validating that the first certificate was signed by the recognized certificate authority.

9. A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method that facilitates secure electronic commerce, comprising:

providing a consumer with a file of security data relating to an account maintained by a financial institution;

creating a financial transaction between the consumer and a merchant, wherein the financial transaction is protected using security data from the file, and wherein the financial transaction is structured to contain an account number in a form that is undecipherable by the merchant, thereby prevent the merchant from knowing the account number for the account;

validating by the merchant that the financial institution identified by the financial transaction is acceptable using security data from the file;

requesting by the merchant that the financial institution authorize the financial transaction;

receiving by the merchant an authorization from the financial institution to complete the financial transaction;

completing the financial transaction between the consumer and the merchant; and

notifying the financial institution that the financial transaction is complete.

10. The computer-readable storage medium of claim 9, wherein the file of security data includes:

a consumer identifier;

a private key for encryption and authentication of data;

a first public key related to the private key for decryption and authentication of data;

an identifier identifying the financial institution;

a second public key belonging to the financial institution;

the account number that has been encrypted with a key known only to the financial institution creating an encrypted account number;

a first certificate signed by a recognized certificate authority that validates the financial institution;

a second certificate signed by the financial institution that validates the consumer; and

computer algorithms to use the file of security data.

11. The computer-readable storage medium of claim 10, wherein the file of security data is provided to the consumer on a smart card.

12. The computer-readable storage medium of claim 11, wherein protecting the financial transaction involves:

creating a first hash of the financial transaction; and

encrypting the first hash, the second certificate, and the encrypted account number using the second public key creating a secure envelope of transaction data, wherein the first hash is created at a secure site available only to the consumer.

13. The computer-readable storage medium of claim 12, wherein requesting by the merchant that the financial institution authorize the financial transaction involves:

creating a second hash of the financial transaction by the merchant;

sending the secure envelope and the second hash to the financial institution;

decrypting at the financial institution the secure envelope using the private key of the financial institution;

comparing the first hash with the second hash; and

if the first hash is identical to the second hash, decrypting the encrypted account number to recover the account number for the account belonging to the consumer,

verifying that the financial transaction is valid for the account, and

if valid, authorizing the financial transaction.

14. The computer-readable storage medium of claim 13, wherein verifying that the financial transaction is valid for the account includes:

verifying that the second certificate was signed by the financial institution;

determining that the account is valid; and

ensuring that a transaction amount is not greater than an authorized transaction amount.

15. The computer-readable storage medium of claim 12, wherein the secure site available only to the consumer is within the smart card.

16. The computer-readable storage medium of claim 10, wherein validating by the merchant that the financial institution identified by the financial transaction is acceptable involves:

receiving at the merchant the first certificate; and

validating that the first certificate was signed by the recognized certificate authority.

17. An apparatus that facilitates secure electronic commerce, comprising:

a providing mechanism configured to provide a consumer with a file of security data relating to an account maintained by a financial institution;

a first creating mechanism configured to create a financial transaction between the consumer and a merchant, wherein the financial transaction is protected using security data from the file, and wherein the financial transaction is structured to contain an account number in a form that is undecipherable by the merchant, thereby prevent the merchant from knowing the account number for the account;

a first validating mechanism that is configured to validate that the financial institution identified by the financial transaction is acceptable using security data from the file;

a requesting mechanism that is configured to request that the financial institution authorize the financial transaction;

a first receiving mechanism that is configured to receive an authorization from the financial institution to complete the financial transaction;

a completing mechanism that is configured to complete the financial transaction between the consumer and the merchant; and

a notifying mechanism that is configured to notify the financial institution that the financial transaction is complete.

18. The apparatus of claim 17, wherein the file of security data includes:

a consumer identifier;

a private key for encryption and authentication of data;

a first public key related to the private key for decryption and authentication of data;

an identifier identifying the financial institution;

a second public key belonging to the financial institution;

the account number that has been encrypted with a key known only to the financial institution creating an encrypted account number;

a first certificate signed by a recognized certificate authority that validates the financial institution;

a second certificate signed by the financial institution that validates the consumer; and

computer algorithms to use the file of security data.

19. The apparatus of claim 18, wherein the file of security data is provided to the consumer on a smart card.

20. The apparatus of claim 19, further comprising:

a second creating mechanism that is configured to create a first hash of the financial transaction; and

an encrypting mechanism that is configured to encrypt the first hash, the second certificate, and the encrypted account number using the second public key creating a secure envelope of transaction data, wherein the first hash is created at a secure site available only to the consumer.

21. The apparatus of claim 20, further comprising:

a creating mechanism that is configured to create a second hash of the financial transaction by the merchant;

a sending mechanism that is configured to send the secure envelope and the second hash to the financial institution;

a decrypting mechanism that is configured to decrypt the secure envelope using the private key of the financial institution;

a comparing mechanism that is configured to compare the first hash with the second hash;

wherein the decrypting mechanism is further configured to decrypt the encrypted account number to recover the account number for the account belonging to the consumer;

a first verifying mechanism that is configured to verify that the financial transaction is valid for the account; and

an authorizing mechanism that is configured to authorize the financial transaction.

22. The apparatus of claim 21, further comprising:

a second verifying mechanism that is configured to verify that the second certificate was signed by the financial institution;

a determining mechanism that is configured to determine that the account is valid; and

an ensuring mechanism that is configured to ensure that a transaction amount is not greater than an authorized transaction amount.

23. The apparatus of claim 20, wherein the secure site available only to the consumer is within the smart card.

24. The apparatus of claim 18, further comprising:

a second receiving mechanism at the merchant that is configured to receive the first certificate; and

a second validating mechanism that is configured to validate that the first certificate was signed by the recognized certificate authority.